**IN THE CLAIMS**

Please cancel claims 1-48 without prejudice or disclaimer as to the subject matter recited therein. Applicant reserves the right to file a divisional application at a later date capturing the subject matter recited in claims 1-48 canceled herein.

1-48 (Cancelled).

49. (Original) A method of community separation control in a Multi-Community Node (MCN), said method comprising:

ensuring routing table compliance with a community separation policy, wherein all routing table updates are validated to ensure said compliance; and

validating a data packet;

allowing further processing of said data packet in response to detecting said data packet is validated; and

discarding said data packet in response to detecting said data packet is not validated.

50. (Original) The method of claim 49, wherein said validating said updates comprises:

determining a network interface through which a next hop corresponding to an update of said updates will be reached;

determining whether a first address corresponding to said next hop is within a first address set of said network interface;

discarding said update in response to determining said destination address is not within said first address set; and

performing said update in response to determining said destination address is within said first address set.

51. (Original) The method of claim 50, wherein said network interface is said determined by either extracting an identification of said network interface from said update or by finding a network interface whose network address prefix matches that of said next hop.

52. (Original) The method of claim 50, wherein said first address is a destination address and said first address set is an Attached Address Set.

53. (Original) The method of claim 50, wherein said first address is a Network Address Community Set (NACS) corresponding to a destination address of said next hop, and wherein said first address set is an Interface Community Set (IFCS) of said network interface.

54. (Original) The method of claim 50, wherein said data packet is an outgoing data packet, and wherein validating said data packet comprises:

determining said destination address is reachable; and
determining a community set corresponding to an interface over which said data packet is to be output includes a community set corresponding to said destination address.

55. (Original) The method of claim 50, wherein said data packet is an incoming data packet, and wherein validating said data packet comprises checking that a source address of said data packet is within an AAS of the interface over which said data packet was received.

56. (Original) The method of claim 50, wherein said data packet is received on a first interface of said MCN and is to be forwarded to a second interface of said MCN, and wherein validating said data packet comprises determining an intersection of an Interface Community Set (IFCS) of said first interface with an IFCS of said second interface is not null.

57. (Original) The method of claim 49 further comprising consulting a Community Information Base (CIB).

58. (Original) The method of claim 57, wherein said CIB includes an IFCS corresponding to each interface of said MCN, and an AAS corresponding to each interface of said MCN indicating destination addresses or destination subnets which are reachable through each of said interfaces.

59. (Original) The method of claim 50, further comprising recording an event corresponding to said update in response to determining said destination address is not within said first address set.

60. (Original) A multi-community node comprising:

a processing unit, wherein said processing unit is configured to ensure routing table compliance with a community separation policy, wherein all routing table updates are validated to ensure said compliance, validate a data packet, allow further processing of said data packet in response to detecting said data packet is validated, and discard said data packet in response to detecting said data packet is not validated; and

a community information base (CIB) coupled to said processing unit.

61. (Original) The node of claim 60, wherein in validating said updates said processing unit is configured to:

determine a network interface through which a next hop corresponding to an update of said updates will be reached;

determine whether a first address corresponding to said next hop is within a first address set of said network interface;

discard said update in response to determining said destination address is not within said first address set; and

perform said update in response to determining said destination address is within said first address set.

62. (Original) The node of claim 61, wherein said network interface is said determined by either extracting an identification of said network interface from said update or by finding a network interface whose network address prefix matches that of said next hop.

63. (Original) The node of claim 61, wherein said first address is a destination address and said first address set is an Attached Address Set.

64. (Original) The node of claim 61, wherein said first address is a Network Address Community Set (NACS) corresponding to a destination address of said next hop, and wherein said first address set is an Interface Community Set (IFCS) of said network interface.

65. (Original) The node of claim 61, wherein said data packet is an outgoing data packet, and wherein in validating said data packet said processing unit is configured to:

determine said destination address is reachable; and

determine a community set corresponding to an interface over which said data packet is to be output includes a community set corresponding to said destination address.

66. (Original) The node of claim 61, wherein said data packet is an incoming data packet, and wherein validating said data packet comprises checking that a source address of said data packet is within an AAS of the interface over which said data packet was received.

67. (Original) The node of claim 61, wherein said data packet is received on a first interface of said MCN and is to be forwarded to a second interface of said MCN, and wherein validating

said data packet comprises determining an intersection of an Interface Community Set (IFCS) of said first interface with an IFCS of said second interface is not null.

68. (Original) The node of claim 60 further comprising consulting said CIB.

69. (Original) The node of claim 68, wherein said CIB includes an IFCS corresponding to each interface of said MCN, and an AAS corresponding to each interface of said MCN indicating destination addresses or destination subnets which are reachable through each of said interfaces.

70. (Original) The node of claim 61, further comprising recording an event corresponding to said update in response to determining said destination address is not within said first address set.

71. (Original) A computer network comprising:

a multi-community node (MCN), wherein said node comprises:

a processing unit, wherein said processing unit is configured to ensure routing table compliance with a community separation policy, wherein all routing table updates are validated to ensure said compliance, validate a data packet, allow further processing of said data packet in response to detecting said data packet is validated, and discard said data packet in response to detecting said data packet is not validated; and

a community information base (CIB) coupled to said processing unit;

a first computer network coupled to said MCN; and

a second computer network coupled to said MCN.

72. (Original) The computer network of claim 71, wherein in validating said updates said node is configured to:

determine a network interface through which a next hop corresponding to an update of said updates will be reached;

determine whether a first address corresponding to said next hop is within a first address set of said network interface;

discard said update in response to determining said destination address is not within said first address set; and

perform said update in response to determining said destination address is within said first address set.

73. (Original) The computer network of claim 72, wherein said node is configured to determine said network interface by either extracting an identification of said network interface from said update or by finding a network interface whose network address prefix matches that of said next hop.

74. (Original) The computer network of claim 72, wherein said first address is a destination address and said first address set is an Attached Address Set.

75. (Original) The computer network of claim 72, wherein said first address is a Network Address Community Set (NACS) corresponding to a destination address of said next hop, and wherein said first address set is an Interface Community Set (IFCS) of said network interface.

76. (Original) The computer network of claim 72, wherein said data packet is an outgoing data packet originating in said MCN, and wherein in validating said data packet said node is configured to:

determine said destination address is reachable; and

determine a community set corresponding to an interface over which said data packet is to be output includes a community set corresponding to said destination address.

77. (Original) The computer network of claim 72, wherein said data packet is an incoming data packet from said first computer network, and wherein validating said data packet comprises checking that a source address of said data packet is within an AAS of the interface over which said data packet was received.

78. (Original) The computer network of claim 72, wherein said data packet is received on a first interface of said MCN and is to be forwarded to a second interface of said MCN, wherein said first interface corresponds to said first computer network and said second interface corresponds to said second computer network, and wherein in validating said data packet said node is configured to determine that an intersection of an Interface Community Set (IFCS) of said first interface with an IFCS of said second interface is not null.

79. (Original) The computer network of claim 71, further comprising consulting said CIB.

80. (Original) The computer network of claim 79, wherein said CIB includes an IFCS corresponding to each interface of said MCN, and an AAS corresponding to each interface of said MCN indicating destination addresses or destination subnets which are reachable through each of said interfaces.

81. (Original) The computer network of claim 72, further comprising recording an event corresponding to said update in response to determining said destination address is not within said first address set.